The Claims

1. (Currently amended) A method implemented at least in part by a computing device, the method comprising:

obtaining ~~generating~~ a manifest that ~~to~~ describes what types of binaries can be loaded into a process space for a trusted application, the manifest comprising:

a first portion including data representing a unique identifier of the trusted application;

a second portion including data indicating whether a particular one or more binaries can be loaded into the process space for the trusted application;

a third portion derived from the data in both the first portion and the second portion by generating a digital signature over the first and second portions; and

a fourth portion that includes data representing a list of one or more export statements that allow a secret associated with the trusted application to be exported to another trusted application;

wherein each of the one or more export statements comprises:

an identifier of the manifest;

an identifier of another manifest that corresponds to the trusted application to which the secret is to be exported; and

a digital signature over both the identifier of the manifest and the identifier of the other manifest; and

using the manifest to control loading of binaries into the process space for the trusted application.

2. (Previously presented) A method as recited in claim 1, wherein the unique identifier of the trusted application comprises:

a public key of a public-private key pair of a party that generates the manifest;

an identifier of the party that generates the manifest; and

a version number of the manifest.

3. (Previously presented) A method as recited in claim 1, wherein the data in the second portion comprises:

a list of one or more hashes of certificates that certify public keys which correspond to private keys that were used to sign the certificates that correspond to binaries that are authorized to execute in the process space.

4. (Previously presented) A method as recited in claim 3, wherein the data in the second portion further comprises:

a list of one or more additional hashes of certificates that certify public keys which correspond to private keys that were used to sign the certificates that correspond to binaries that are not authorized to execute in the process space.

5. (Previously presented) A method as recited in claim 1, wherein the data in the second portion comprises:

a list of one or more certificates that certify public keys which correspond to private keys that were used to sign the certificates that correspond to binaries that are authorized to execute in the process space.

6. (Previously presented) A method as recited in claim 5, wherein the data in the second portion further comprises:

a list of one or more additional certificates that certify public keys which correspond to private keys that were used to sign the certificates that correspond to binaries that are not authorized to execute in the process space.

7. (Previously presented) A method as recited in claim 1, wherein the data in the second portion comprises:

a list of one or more public keys which correspond to private keys that were used to sign the certificates that correspond to binaries that are authorized to execute in the process space.

8. (Previously presented) A method as recited in claim 7, wherein the data in the second portion further comprises:

a list of one or more public keys which correspond to private keys that were used to sign the certificates that correspond to binaries that are not authorized to execute in the process space.

9. (Canceled).

10. (Canceled).

11. (Previously presented) A method as recited in claim 1, wherein at least one of the one or more export statements comprises:

an identification of a particular computing device on which the at least one export statement is useable.

12. (Previously presented) A method as recited in claim 1, wherein the data structure further comprises:

an additional portion that includes data representing a set of properties corresponding to the data structure.

13. (Previously presented) A method as recited in claim 12, wherein the set of properties includes:

whether the trusted application is debuggable.

14. (Previously presented) A method as recited in claim 12, wherein the set of properties includes:

whether to allow an additional binary to be added to the process space after the trusted application begins executing.

15. (Previously presented) A method as recited in claim 12, wherein the set of properties includes:

whether to allow implicit upgrades to a higher version number.

16. (Previously presented) A method as recited in claim 1, wherein the data structure further comprises:

an additional portion that includes data representing a list of entry points into the executing trusted application.

17-76. (Canceled).